Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 128 (2015) 54 – 63

Procedia Engineering

www.elsevier.com/locate/procedia

3rd European STAMP Workshop, STAMP EU 2015

The integration of drones in today's society

Mitchel Pappot[a], Robert J. de Boer[a]*

[a]*Amsterdam University of Applied Sciences, Aviation Academy, Weesperzijde 190, 1097 DZ Amsterdam, the Netherlands*

Abstract

The integration of Remotely Piloted Aircraft Systems (RPAS) in today's society depends on the ability of their operators to demonstrate safety. RPAS operators use risk matrices, as required by the Dutch government, to indicate the safety level. Key issues with this approach include the lack of available component reliability data for determining the risk factors, and the exclusion of human interactions. This study aims to determine the competence of the Systematic Theoretic Process Analysis (STPA) to demonstrate the safety of RPAS operations. It is concluded that the STPA is a comprehensive method to demonstrate the safety of RPAS operations.

Peer-review under responsibility of the organizing committee of STAMP EU 2015

Keywords: civil RPAS; civil Drones; STPA; STAMP; safety; systems theory; risk matrices

1. Introduction

Remotely Piloted Aircraft Systems (RPAS) are increasingly used for private and business needs. Because of recent developments in regulations related to the operation of business RPAS, the market now sees a great potential in the use of RPAS for commercial and civil purposes. However, the permission to use professional RPAS is highly dependent on the ability of the operator to demonstrate the safety of these operations to the authorities, and therefore on the type of operation. RPAS operated within the borders of the European Union (EU) are divided into two weight categories: 'Light' RPAS with a gross weight up to 150 kg which are controlled by local government authorities in the specific country of operation; and 'heavy' RPAS with a gross weight above 150 kg that are regulated by the EASA [1]. Light RPAS have been found to be particularly suitable for civil operations. RPAS have already been used for

* Corresponding author. Tel.: +31618561188
E-mail address: M.K.Pappot@hva.nl

Peer-review under responsibility of the organizing committee of STAMP EU 2015
doi:10.1016/j.proeng.2015.11.504

aerial cinematography, ground mapping, crop inspections and the inspection of windmill blades. Other applications, such as crowd control, surveillance, chemical detection and firefighting are of interest for commercial RPAS manufacturers and operators but are severely restricted in the interest of public safety.

Current safety assessment techniques used to determine the safety of RPAS in civil operations are based upon the identification of hazards and classification of the risk for each identified hazard. The current methodology mainly reasons from the failure or inadequate functioning of individual components that might result in accidents. Human errors, software errors and external disturbances are generally not considered during the analysis. However, new methods based on systems thinking have recently become available that do incorporate interactions between system components and potentially identify flaws in human performance, in software and due to external disturbances. One such approach is Systematic Theoretic Process Analysis (STPA).

The aim of this study is to investigate the ability of STPA to demonstrate the safety of light RPAS operations for business and determine whether the STPA is a more preferable analytical method compared to the current hazard identification and risk matrix safety analysis method used by the RPAS industry. To do so, the STPA and the current methodology are applied to case studies in the context of civil RPAS operations.

2. Background

2.1. STAMP / STPA

STAMP is a safety model based on systems theory. Unlike the traditional safety assessment methodologies STAMP does not use a chain of event model to describe the occurrence of accidents [2]. Instead, safety models based on systems theory consider accidents as a result of interactions between components; they do not represent a single cause for an accident, but reveal multiple factors - variables that collectively contribute to an accident [3]. STAMP views safety as a control problem and supports that accidents do not merely occur from component failures. Instead, accidents occur because of inadequate enforcement of safety constraints, inadequate control of system components or external disturbances considering the interactions between people, organizational structures, and the physical system components [4]. STAMP contemplates the system to be in a state of dynamic equilibrium. The equilibrium state is established by the control and feedback links among components. Viewing the process as a dynamic state means that the system adapts to internal and environmental changes. STAMP is based on three stages: defining the safety constraints, generating a hierarchical control structure and developing a systemic process model [5].

2.1.1. Safety constraints

STAMP embeds the concept of imposing constraints on a system's degrees of freedom [6]. An accident or loss is the result of inadequate enforcement of safety constraints rather than a single failure resulting in a loss or accident. Constraints can be applied during the design and operation of a system, to ensure safe system behaviour. Constraints are derived from the purpose and functions of a system. Enforcement of safety constraints is necessary to prevent the system moving towards a hazardous state. A person or organisation that places constraints on another level of the system also needs some form of feedback to be able to reflect on the effectiveness of the safety constraints [4].

2.1.2. Hierarchical control structure

A system can be represented graphically as a hierarchical control structure. The aim of a hierarchical control structure is to identify the system components, facilitate the generation of safety constraints and depict the feedback loops within the system [2]. Each level in the hierarchical control structure imposes constraints on the level below it. Constraints for each level of the structure can include design, process, operational, manufacturing and managerial constraints [7]. Constraints - when related to safety - specify the relationships between system variables that contribute to the safe state of the system [6]. The hierarchical control structure consists of two basic structures with communication links between them. The first part consists of the system development structure, where levels impose constraints on the design and development of the system. The second part of the structure is dedicated to the operation of the system [8]. Although a basic hierarchical control structure consists of the development and operational control structure, additional structures can be added to the model when these carry the responsibility of enforcing the safety of another part of the system [2].

Within the hierarchical control structure, two forms of information flow can be found: 1) Constraints and communication channels provide information from higher levels to lower levels, and 2) Feedback loops provide feedback about the effectiveness of safety constraints from the process to the control levels. Flaws such as the absence of communication and feedback or lack of timeliness can result in inadequate control. Inadequate controls include missing feedbacks to higher levels and incorrect executions of control actions within lower levels of the system [2]. Since STAMP considers the system to be in a state of dynamic equilibrium, the efficiency of the control structure in enforcing and developing safety constraints can be affected by delays in communications between the levels [5]. Communication from higher located levels may take too long to effectively enforce safety constraints. Particularly in technological environments that change rapidly, lower levels bear the responsibility for integrating safety constraints and information from higher levels within the current state of the system [2].

2.1.3. System control structure

Every controller within the system contains a control algorithm, which determines the control actions that need to be taken [2]. For a human controller, the control algorithm is usually referred to as the 'mental model', which includes assumptions regarding the state of the process being controlled. The controller is responsible for enforcing safety constraints and issuing control actions to change the system's behaviour to maintain safe operation [6]. A controller executes control actions using actuators. The actuator translates the control action into an input for the process. The controller receives feedback via sensors that measure characteristics of the process. It is also possible for a process to be controlled via multiple controllers. Those controllers must share a similar process model of the system to be able to provide adequate control [9]. If the controllers provide conflicting control actions, the system's behaviour may be negatively affected. It is therefore important to develop common awareness of the state of the system amongst the controllers, so that inadequate or unsafe control actions are eliminated [2, 8].

2.1.4. STPA, Using the control structure to identity unsafe control actions

STPA is a safety analysis method based on the STAMP model. The goal of STPA is to determine how unsafe control actions might occur within the system and identify safety constraints to prevent unsafe control actions from being issued. Before executing STPA it is first necessary to identify the system hazards and accidents to be prevented, and develop a system control structure. The first step of the STPA is to define the unsafe control actions. The STPA describes five categories of unsafe control actions that can contribute to hazards [2]:

1. A control action required for safety is not provided.
2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied for too long (for a continuous or non-discrete control action).
5. A required control action is provided, but not followed.

Unsafe control actions that are linked to predetermined system hazards can be used to modify the control structure by adding safety constraints and/or feedback, thus mitigating the unsafe control actions. It is important to note that control actions are only valid or dangerous in a certain context. It is therefore important to define the context and its associated conditions [2]. A relevant systematic method has been created by Thomas [10]; this method defines unsafe control actions in an organized way, so that the controller, actions and context are included. The identified unsafe control actions can be translated into safety constraints. The aim of defining safety constraints is to impose restriction on the system's behaviour in order to prevent the unsafe control actions and their consequences from occurring.

2.1.5. Reviewing the control structure to identify the causes of unsafe control actions

Having identified the unsafe control actions and safety constraints the next step is to determine how unsafe control actions can be issued or how safe control actions can be executed unsafely. Unsafe control actions or inadequate execution of control actions can lead to a single cause or multiple causes scenarios which, when combined, provide a condition in which the system moves towards a hazardous state [6]. All causes and scenarios provide information that can be used to create new safety constraints or conditions, with the aim of preventing the unsafe control actions from happening. Within this process, human errors and software errors are similarly denoted, and can both be affected in a similar way [2].

2.2. Current safety analysis methodology for professional RPAS operations

Professional RPAS operators are required to prepare a safety analysis before each operation. The safety analysis is part of the flight plan procedure and must be approved by the authorities before being able to legally operate. The Dutch Civil Aviation Authority (NL-CAA) proposed to use brain storm sessions and to include experience from past operations to identify the hazards of a particulair RPAS operation [11]. Once the hazards are identified risk matrices are used to determine the risk of a hazard.

Operational experts that identified the hazards during the brainstorm session determine the severity of a hazards based on their own experiences. Keeping in mind the consequences for the operational ability of the RPAS, as well as the consequences for the direct environment and safety of people and aircraft [12]. The severity of the hazard can be classified in five categories; catastrophic, hazardous, major, minor or negligible.

To determine risk probability, operators classify the rate of occurrence from their previous experiences. The likelihood of a hazard is also classified in five categories: Frequent (the hazards occur several times per year); occasional (the hazard arises a couple times per year); remote: (the hazard occurs once or twice a year); improbable (the hazards has not appeared earlier); and extremely improbable (almost inconceivable that it will ever occur).

The risk of a hazard is the product of the likelihood and severity. Whenever a hazard has a high risk factor the authority will not approve the flight plan unless effective mitigation measures are taken. When all of the hazards that were identified have been mitigated to an acceptable level of risk, the analysis shows that the operation is safe to be executed.

3. Research Method

This study is based upon the STPA methodology of Leveson [2] and Thomas [10] and risk matrix methodology of the VMS light [11, 12]. Both methodologies were applied to case studies based on civil RPAS operations. STPA proves to be a suitable tool if the comparison of the results from both analysis methodologies shows that at least all risks and hazards found by using the risk matrix methodology are found by using the STPA. The latter proves to be a more comprehensive methodology to demonstrate the safety of RPAS operations if, and to the extent that, any of the following apply:

1. STPA identifies more hazards, including all the hazards found using the current methodology
2. STPA identifies the same hazards, but describes them better, enabling a better operational understanding
3. STPA identifies hazards in less time
4. STPA provides additional perspectives of the operation which are not included in the current methodology
5. STPA provides more guidance for the analyst compared to the guidance provide to use the current methodology.

4. Case study description

During the study four RPAS application cases for business were assessed by the traditional risk matrix analysis and STPA. A generic RPAS model was developed as a foundation of the system used in the case studies. Case study requirements were identified during a literature survey on RPAS regulations. Further detail and context of the RPAS operations were developed with the use of business RPAS operators from the Netherlands. Each of the four case studies present different types of operation and technological complexity. The first case represents a manually controlled RPAS flying in line of sight of the pilot and carrying a camera controlled by a secondary pilot. The second case is similar to the first operation only the complexity level of the RPAS is increased by adding sensors and flight modes such as ‘altitude hold’ to aid the pilot flying. Also an additional observer is present to allow the RPAS to fly further away from the pilot. The third case presents a beyond line of sight operation whereby the pilot and secondary pilot depend on technology to provide a live image from the RPAS. The fourth case represents a RPAS capable of flying a pre-programmed route without active input from the pilot.

5. Application of the STPA

5.1. *System foundation*

The foundation for STPA is the definition of hazards that might lead to an accident. For business RPAS, three accidents are defined: (1) RPAS collides with objects and persons on the ground, (2) RPAS collides with airborne objects (aircraft), and (3) the mission objective fails. After defining the system accidents the hazards that contribute towards or induce the accidents are defined (Table 1).

Table 1. Identified hazards

ID	Description	Links to accidents
H1	RPAS collides with terrain due to control actions (controlled flight)	A1, A3
H2	RPAS control is entirely lost	A1, A2, A3
H3	RPAS / camera data connection is lost or not recorded	A3
H4	RPAS is launched or remains flying without permission	A1, A2
H5	RPAS violates the safety separation limits	A1, A2
H6	RPAS damages surroundings, causes injury to humans, or is damaged during take-off or landing	A1, A2, A3

Before initiating the STPA, a control structure representing the system of interest is required. The control structure for the operating process consists of four components: the RPAS pilot, the remote control system, the physical RPAS and the ground station (Fig. 1a). The RPAS pilot acts as a controller and issues the control actions. The pilot operates using a control algorithm based on the current state of the system, the set point for the system, the desired behaviour of the system and his/her responsibilities. The pilot is responsible for the safety of the operation and must adhere to airspace safety restrictions, the physical limits of the RPAS and its operational requirements. These requirements and limits are available to the pilot in his so-called process model. Not all decisions are issued based on feedback alone: the process model includes assumptions regarding the operation of the controlled process and its current state. The pilot receives feedback from various sensors in the control structure to re-establish his/her awareness of the current state of the system. In general, the pilot receives feedback via two sensors: visual cues from the RPAS, and information from the observer (i.e. a compulsory second person). The pilot controls the RPAS via a remote control system (i.e. actuator). This remote control system communicates directly with the RPAS. The RPAS is part of the controlled process. The RPAS receives control input from the remote control system, and acts on the input. Furthermore, the RPAS relies on power from the battery to operate. Other external factors like the wind can affect RPAS operation and control. The RPAS, in turn, provides through sensors information about its current state.

Three out of four case studies were based upon this generic control structure. However, the fourth case study covered the most complex system and type of operation: a semi-automated operation. In this case, the RPAS flies a pre-defined route which is stored inside RPAS’s memory. The only input needed for the operation is the take-off command, which has to be provided by the pilot. Furthermore, the pilot is able to take manual control in case of an emergency and receives real-time feedback from the RPAS. For this case, a more advanced control structure was needed to cover the complexity of the system (Fig. 1b).

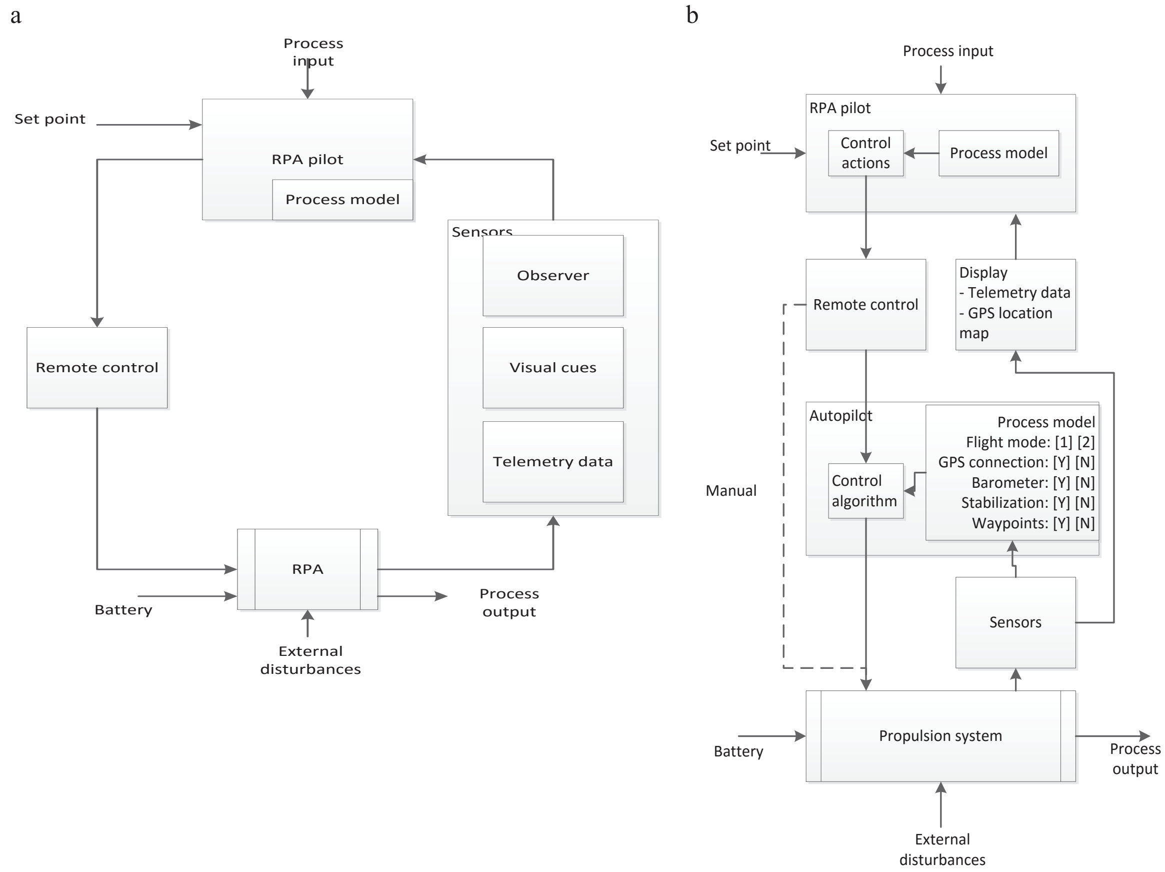

Fig. 1. (a) Generic control structure for case 1 -3; (b) Advanced control structure for case 4

5.2. *Assumptions*

For the initial STPA it was assumed that:

1. The system has been configured of elements that are airworthy.
2. The RPAS is certified in compliance with Dutch standards.
3. The operational manual, including the operating procedures, have been drawn up in compliance with Dutch standards and approved.
4. The RPAS pilot has received and maintained his/her pilot's licence.
5. The observer and RPAS pilot have adequate knowledge of RPAS operations as required by the operator.
6. The RPAS is designed by a company which possesses a 'Design Organisation Approval'.
7. The RPAS is built by an organisation which possesses a 'Production Organisation Approval'.
8. The RPAS is maintained by a qualified organization which possesses a 'Maintenance Organisation Approval'.

5.3. *STPA step 1*

The first step in the STPA process is to identify the unsafe control actions. Not all unsafe control actions provide unique hazards and some control actions contribute to several similar hazardous system states. Therefore, the identified unsafe control actions were revised in order to link the unsafe control actions to unique hazardous control states. By using the hazardous control states identified, the safety constraints were developed [2].

5.4. STPA step 2

The second step of the STPA analysis is to develop scenarios and identify causal factors that explain how unsafe control action can be issued. An example of the identification of scenarios and causal factors for the following hazardous control state "RPAS takes-off whilst take-off authorization is not provided" is presented.

Hazard:

The RPAS initiates take-off procedure whilst take off authorization is not provided (permission not granted, or take off area not cleared of objects).

Associated Safety constraints:

1. The RPAS shall not take off without input from the pilot.
2. The pilot shall not issue the take-off command without proper authorization.

Next, the causal factor analysis aims to identify how the unsafe control actions or a combination of unsafe control actions can be issued and result in the unauthorized take off of the RPA. A total of 28 scenarios and 109 associated causal factors were identified for this case. An example of the causal factors identified for the identified hazard 'RPAS takes-off whilst take-off authorization is not provided' is presented in Fig. 2, where we show five of the identified causal factors that solely or in combination with other causal factors might lead to this hazardous system state. In this example it is apparent that causal factors exist at all levels of the system and can also be inflicted by input from outside the system. A pilot that receives conflicting, missing information regarding take off permissions, or misinterprets it, might proceed to an unauthorized take off of the RPAS. The autopilot is also able to initiate take off when the 'arm' command is provided whilst the autopilot is in automated flight mode or when it receives inadequate feedback from the altitude sensors providing the autopilot with a non-zero altitude or vertical speed.

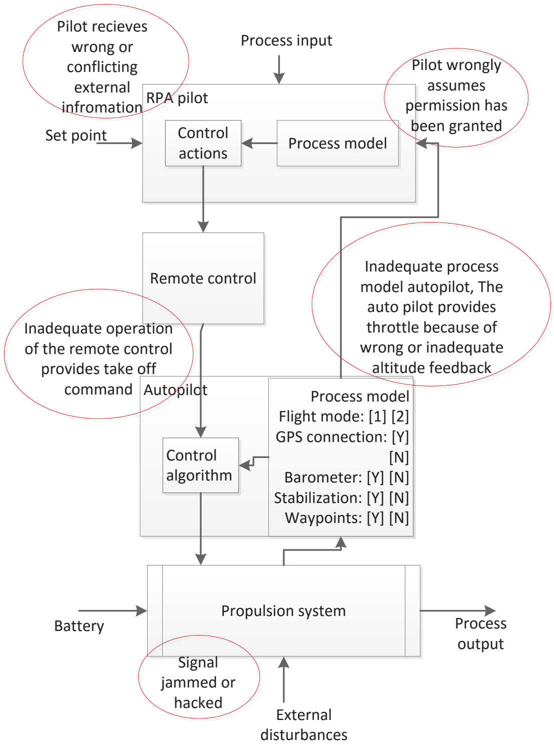

Fig. 2. Example of causal factors HSC-2

6. Results of the STPA and risk matrices methods

6.1. Results from the risk matrices

The risk matrices were used to determine the risk of the hazards identified during the brainstorm for each case. Also the consequences in terms of the RPAS ability to maintain flight and increase of pilots' task load were identified for each hazard. The risk matrices divided the hazards in acceptable hazards and high priority hazards. An increase in system and operational complexity manifests itself by an increased number of identified hazards and failure modes within the control software and autopilot, the sensor system, and piloting station. Although the fourth case has the highest system complexity, fewer hazards could be identified. This can be explained by the lack of an operational camera system; this type of RPAS is equipped with a chemical sniffer, which is a static load independent of the RPAS and is not controlled during the operation and eliminates the need for an operator.

6.2. Results from the STPA

The feasibility of using the STPA for determining the safety of light RPAS operations for business has been demonstrated by the application of STPA to these cases. Having established the general foundations of the STPA including the assumptions, the common hazards, common accidents and general control structure, each case was subjected to the STPA. Some control actions were found to contribute to similar hazards, and were merged into hazards control states on which safety constraints were developed. The STPA analysis for each case was stopped when all possible scenarios had been identified and analysed, and mitigation measures were found.

6.3. Comparison between STPA and risk matrices and related work

To compare the results from the risk matrices with the ones from the STPA, the causal factors and hazards identified by both methodologies were assessed. The comparison showed that risk matrices do not incorporate the effect of delays throughout the system, do not identify inconsistent process models and do not identify the effects of missing communication lines. This can be explained by the approach used to identify the hazards: in traditional methods risks are identified based on linear methods (e.g., FTA, FMEA) which focuses on component failures, and generic models (SHELL, 5M) that rely on previous knowledge and experience. Because of this, traditional methods do not focus on the interactions between components. STPA however, considers the communications and interactions between components and levels of the system.

External influences, such as air pollution and moisture that could affect the RPAS were not identified by STPA as being hazards. However, STPA does allow for process disruptions and therefore did account for the influence of adverse weather conditions and other external disturbances on the operational ability of the RPAS as they arise in different scenarios.

7. General Results

The requirements for determining the competence of the STPA to demonstrate the safety of RPAS operations were developed in the methodology of the study. They are now compared to the results of the analysis.

- *STPA identifies more hazards, including all the hazards found using the current methodology*

The comparison of results showed that STPA is capable of identifying all hazards identified by the risk matrices. Moreover, the STPA identified more hazards that were not identified using the current methodology. There is, however, a difference in the classification of hazards. The hazards identified by the current methodology that include environmental conditions were identified by the STPA as external influences on the system. This is different from the current methodology that classifies the external influences as hazards. However, the influence of external factors are present in several scenarios of the STPA.

- *STPA finds the same hazards, but describes them better, which allow for a better operational understanding*

Risk matrices describe failure mode effects in terms of the operational ability of the RPAS and increased task load of the pilots [13]. STPA identified scenarios and associated causal factors that explained how hazards can occur [2]. Both analyses presented causal factors that contributed to hazards. STPA, however, described how a set of conditions can result in a hazard.

- *STPA identifies hazards in less time*

Both analytical techniques are iterative and depend upon the expertise of the analyst. The analyses were developed over a long time period, as the analyst needed to review both analytical techniques. Which analytical method takes longer cannot therefore be concluded.

- *STPA provides additional perspectives that are not included in the current methodology*

The comparison revealed that STPA analysis strengthens safety analysis by including the interactions between components of the system. The interaction between controllers and system components is not covered by the risk matrices. Furthermore, STPA reveals how hazards can emerge due to the failure or degradation of components. Risk matrices based on traditional methods reason from a failure that includes *either* the failure *or* inadequate operation of a component within the system. Thus, risk matrices do not reveal how hazards emerge without component failures.

8. Conclusions

With the introduction of new regulations for business RPAS operations, a new era for RPAS operators has arrived. However, the increase in RPAS operators and operations could adversely affect safety. Therefore, the development of risk analysis methods for demonstrating the safety of RPAS operations has become important. This paper attempted to examine the competence of STPA to demonstrate the safety of professional category 1 RPAS during fictional class 2 operations.

The results showed that STPA presents a different approach to analysing hazards. Risk matrices examine the implications of a failure, and therefore focus on failure modes. The interactions between components in particular, including delays and process model inconsistencies were only identified by the STPA. The scenarios and associated causal factors identified during STPA provided the analyst with the detailed information necessary to develop effective mitigation measures. The comparison showed that STPA is suitable for identifying all risks and causal factors identified by risk matrices. Moreover, STPA identified more causal factors that were linked to scenarios for each of the cases analysed.

For high priority hazards mitigation measures taken by operators currently focus on redundancy, since the most common problem with RPAS is the lack of reliability data. Currently the regulatory bodies are moving towards similar requirements for redundancy in RPAS systems. This includes adding back-up systems to the RPAS which entails the increase in system complexity.

Business RPAS operators are expected to benefit from the use of the STPA method to analyse the safety of professional RPAS operations in the future. Since business operated RPAS is a fairly new profession the STPA proves to be useful to identify the hazards that could arise not only due to system failures but also due to ineffective controls or miscommunication. STPA can help operators to define safety requirements and safety responsibilities for the operational RPAS crew. The additional identified hazards therefore provide new insight that is currently not accounted for by the current methodology. However, the quality and quantity of the hazards identified with the current methodology is highly depended on the expertise of the operators. Operators that have previous knowledge with other safety analysis methods might be capable of using that knowledge and applying it to the current method. Therefore, the results from the safety analysis using the current methodology might vary.

The STPA was shown to be a well-guided process that provides scenarios and identifies causal factors that can be used to develop more effective mitigation measures compared to the current methodology. However the identification process of mitigation measures shows to be the hardest part of the STPA since there is less guidance available for this process.

References

[1] EASA, Remotely Piloted Aviation Systems (RPAS), European Aviation Safety Agency, Brussels, 2014.
[2] N.G. Leveson, An STPA Primer, http://sunnyday.mit.edu/STPA-Primer-v0.pdf (accessed 12 August 2015).
[3] J. Leplat, Occupational accident research and systems approach, in: J. Rasmussen, K. Duncan, J. Leplat (Eds.), New Technology and Human Error, John Wiley & Sons, London, 1987, pp. 181–191.
[4] N. Leveson, M. D. Daouk, K. Marais, Applying STAMP in Accident Analysis, MIT, Boston, 2003.
[5] M. Placke, Application of STPA To The Integration Of Multiple Control Systems: A Case Study And New Approach, Master Thesis, MIT, Boston, 2012.
[6] N.G. Leveson, Engineering A Safer World: Systems Thinking Applied to Safety, MIT Press, Cambridge, MA, 2011.
[7] N. Leveson, A new accident model for engineering safer systems, Safety Science. 42 (2004) 237–270.
[8] Y. Song, Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis, Master Thesis, McMaster University, Hamilton, Canada, 2012.
[9] T.L. N. Ishimatsu, N. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, H. Nakao, Modeling and Hazard Analysis Using STPA, MIT, Boston, 2015.
[10] J. Thomas, Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis, PhD Thesis, MIT, Boston, 2013.
[11] The Human Environment and Transport Inspectorate, Safety Management, Netherlands, 2011.
[12] The Human Environment and Transport Inspectorate, Informatiebulletin lichte onbemande luchtvaartuigen UAS – Unmanned Aircraft Systems, Netherlands, 2015.
[13] JARUS, Remotely Piloted Aircraft Systems Safety Assessment, Scoring Paper to AMC RPAS.1309, EASA, Brussels, 2014.